

AFFIDAVIT OF SPECIAL AGENT KATRINA P. CAULFIELD

I, Katrina P. Caulfield, state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (“USSS”) and have been employed as such since August of 2021. I attended the United States Secret Service Special Agent Training Course at the James J. Rowley Training Center in Beltsville, Maryland. I am currently assigned to the Boston Field Office where I conduct financial crime investigations, including investigations of violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1956 (Money Laundering). In connection with these investigations, I have conducted or participated in numerous field interviews of suspects and witnesses, electronic and physical surveillance, researched bank account documents and documents relating to the wiring of monies between banks. Through my training and experience, I have become familiar with various financial frauds and schemes such as bank frauds, wire frauds and mail frauds.

PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of a Verified Complaint for Forfeiture *in Rem* against the following cryptocurrency seized from Binance account associated with User ID XXXXX3280 (“ACCOUNT 1”) on or about October 25, 2024:

- a. 7.23918814 BTC¹;
- b. 105.75351403 ETH²;
- c. 636.11899592 AVAX³;

¹ “BTC” is the abbreviation for Bitcoin, a blockchain-based cryptocurrency with its value to dollar fluctuating with the market.

² “ETH” is the abbreviation for Ethereum, a blockchain-based cryptocurrency with its value to dollar fluctuating with the market.

³ “AVAX” is the abbreviation for Avalanche, a form of cryptocurrency.

- d. 14120.995091 USDT⁴;
- e. 2380467906.17 SHIB⁵ ; and
- f. 319008151.01 PEPE⁶

(collectively, the “Defendant Property”).

3. As set forth below, there is probable cause to believe that the Defendant Property represents proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud) and is property involved in violations of 18 U.S.C. § 1956 (Money Laundering) and is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C). The Defendant Property was seized pursuant to a seizure warrant issued in the District of Massachusetts on June 18, 2024, and was subsequently transferred to government-controlled wallets.

4. This affidavit is based on my personal knowledge, information provided by other law enforcement offices and government employees, and information gathered during this investigation including interviews of witnesses, the review of documents, and conversations with other law enforcement officers. This affidavit is not intended to set forth all of the information that I have learned during this investigation but includes only the information necessary to establish probable cause for the forfeiture of the Defendant Property.

BACKGROUND ON CRYPTOCURRENCY

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

6. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to

⁴ “USDT” is the abbreviation for Tether, a form of cryptocurrency whose tokens operate as stablecoin, indicating that each token is equivalent in value to one U.S. dollar.

⁵ “SHIB” is the abbreviation for Shiba Inu, a form of cryptocurrency.

⁶ “PEPE” is memecoin, a form of cryptocurrency.

buy goods or services or exchanged for fiat currency or other cryptocurrencies.⁷ Examples of cryptocurrency are Bitcoin (BTC), Litecoin, and Ether (ETH). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.⁸ Cryptocurrency is not illegal in the United States.

7. Bitcoin⁹ is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (*i.e.*, online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people.

Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins

⁷ Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

⁸ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

⁹ Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it is not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

8. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

9. Although cryptocurrencies such as Bitcoin and Tether have legitimate uses, like fiat currencies, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

10. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (*e.g.*, smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their

cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

11. Cryptocurrency “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether. According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.¹⁰ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are frequently able

¹⁰ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

12. Binance Capital Management Co., Ltd. (“Binance”) is a cryptocurrency exchange and custodian that allows users to buy, sell and store digital assets. They hold a Money Service Business Registration in the United States. Binance receives service through Nest Services Limited. Their registration shows an address of House of Francis, Room 303, Ile Du Port, Mahe, Seychelles.

13. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users’ funds or the private keys that are necessary to access users’ wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users’ cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user’s wallet directly, such as by accessing the user’s smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

PROBABLE CAUSE

14. As set forth below, there is probable cause to believe that the Defendant Property represents proceeds obtained through violation of 18 U.S.C. § 1343 (Wire Fraud) and/or is property involved in violation of 18 U.S.C § 1956 (Money Laundering).

15. Pursuant to 18 U.S.C. § 981(a)(1)(C), property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, specifically violations of 18 U.S.C. § 1343 (Wire Fraud), is subject to civil forfeiture. Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(c)(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity. It is a violation of 18 U.S.C. § 1343 for a person to devise and intend to devise a scheme and artifice to defraud for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud.

16. Pursuant to 18 U.S.C. §§ 981(a)(1)(A), property, real or personal, involved in a transaction or attempted transaction, here, violations of 18 U.S.C. § 1956(a)(1)(B)(i) and (h) (money laundering and conspiracy to commit money laundering) or property traceable to such property is subject civil forfeiture. It is a violation of 18 U.S.C. § 1956(a)(1)(B)(i) (laundering of monetary instruments) to conduct or attempt to conduct a financial transaction knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of a specified unlawful activity. It is a violation of 18 U.S.C. § 1956(a) to conspire to engage in the offense of money laundering.

The Scheme to Defraud

17. On or around March 15, 2024, Victim-1 of Newton, Massachusetts completed an Internet Crime Complaint Referral Form through the Internet Crime Complaint Center¹¹ providing information indicating she was the victim of a cryptocurrency trading scam. Between March 28, and April 22, 2024, I communicated with Victim-1 via telephone and email. Victim-1 explained on or around February 2024 she initially joined a Facebook Group named “Financial Independence Forum.” The Facebook Group purports to be a “community dedicated to assist individuals achieve financial independence and early retirement through reliable investment.”

18. After connecting with various individuals through the Facebook Group, Victim-1 contacted an individual named “TOM SHELDON HALEY” through Facebook Messenger on February 24, 2024. The individual or individuals purporting to be “TOM SHELDON HALEY” communicated with Victim-1 through the messaging application, Facebook Messenger. Victim-1 received communications on this messaging applications from “TOM SHELDON HALEY” who utilized a phone number ending in 9972. Victim-1 also utilized the website “[https://tomsheldonhaley\[.\]com/](https://tomsheldonhaley[.]com/)” to contact “TOM SHELDON HALEY.”

19. Victim-1 provided investigators with screenshots of her communications with “TOM SHELDON HALEY.” The screenshots show messages typed in English, which I reviewed.

20. The individual or individuals purporting to be “TOM SHELDON HALEY” are the administrators of the “Financial Independence Forum” Facebook Group. “TOM SHELDON HALEY” introduced Victim-1 to a cryptocurrency exchange that Victim-1 believed to be Trade

¹¹ The Internet Crime Complaint Center or IC3 is the United States’ central hub for reporting cybercrime and is run by the Federal Bureau of Investigation.

Propel. “TOM SHELDON HALEY” and other individuals in the Facebook Group, “Financial Independence Forum,” posted within the group screenshots showing “profit gains” by investing in cryptocurrency.

21. “TOM SHELDON HALEY” sent Victim-1 multiple messages claiming his “expertise in investments and effective trading strategies”. Victim-1 stated she followed “TOM SHELDON HALEY’s” instructions and transferred funds to her existing Coinbase wallet. Victim-1 then created an account for an exchange “Tradepropel[.]com.” “TOM SHELDON HALEY” provided Victim-1 a website URL of “tradepropel[.]com,” which she was told was an automated trading system platform. “TOM SHELDON HALEY” sent Victim-1 screenshots and detailed instructions of the steps to take on the website to create an account and transfer funds into the Trade Propel platform.

22. Victim-1 made her first transaction to Tradepropel[.]com on March 15, 2024 with “TOM SHELDON HALEY’s” help. After this initial transaction, when Victim-1 visited the website, she saw profit gains within her Trade Propel account.

23. “TOM SHELDON HALEY” informed Victim-1 that Trade Propel was an automated trading system therefore no manual investments other than funding the account was necessary. “TOM SHELDON HALEY” stated once Victim-1 added more funds to the account, he would devise a new strategy for investment.

24. As evidenced by Victim-1’s messages and financial records, which I have reviewed, between February 24, 2024 and March 14, 2024, the individual or individuals identifying themselves as “TOM SHELDON HALEY” instructed Victim-1 to transfer 1.33272285 BTC to a cryptocurrency wallet on Trade Propel. Victim-1 stated she bought BTC

on Coinbase.com and sent one cryptocurrency transfer from her account at Coinbase.com to the destination wallet address detailed below. Victim-1 also provided details of this transfer.

25. I conducted a review of the transfer details provided by Victim-1 and was able to verify the cryptocurrency transfer totaling 1.33272285 BTC transferred out of Coinbase.com.

26. Victim-1 stated she conducted the cryptocurrency transfer from her account at Coinbase.com under the direction and instructions she received from “TOM SHELDON HALEY”.

27. Victim-1 stated that on March 14, 2024, she tried to withdraw money from the “Trade Propel” website but had received a message from customer service and was instructed that she needed to pay “tax on earnings” in her account. These instructions caused Victim-1 to question the legitimacy of “Trade Propel”. Based on my training and experience, I know that scammers often attempt to extract additional funds from victims by instructing victims to pay “taxes” to the scammers before the victims can withdraw funds.

28. Victim-1 provided screenshots of the “Trade Propel application” appearing to show a cryptocurrency portfolio, including a cryptocurrency deposit history and trading history. Screenshots provided by Victim-1 also appeared to indicate gains and losses of cryptocurrency portfolio value.

29. I conducted a thorough open source search for ‘Trade Propel’, and as of May 8, 2024, it is not an exchange listed or operating within the United States.

30. I conducted a thorough open-source search for the URL “[https://tradepropel\[.\]com](https://tradepropel[.]com)” and was able to identify and access the website which Victim-1 indicated she visited. Based on my training and experience, as well as conversations with other investigators familiar with cryptocurrency platforms, I would expect a legitimate cryptocurrency

platform website to be accessed through a web browser and contain clearly outlined platform policies, company contact information, information regarding the platform's creation, company staff information, along with access for desktop and mobile computing. Upon navigating to the website, I observed the website was missing the above information. It contained introductory bios of George Soros, Paul Tudor and Ray Dialo, alluding to the fact these widely known billionaire hedge fund managers co-sign the use of this platform. There are numerous “customer” reviews that do not appear to be legitimate customers. Also, the website falsely claims to be part of FINRA and SIPC. All of these items combined, and my training and experience, makes me conclude that the creator of the website was trying to create the impression of legitimacy to gain the trust of any potential “customer.”

31. In addition, when conducting open-source research on scams related to the Trade Propel platform, I identified multiple websites indicating this platform was a “scam.” Furthermore, I was able to identify additional law enforcement reports detailing similar scams utilizing Trade Propel and “Financial Independence Forum” Facebook Group.

32. Based on my training and experience, the discrepancies identified above are not typical for a legitimate cryptocurrency platform.

33. Accordingly, I have probable cause to believe Victim-1 was fraudulently induced to transfer funds to a scam cryptocurrency platform, *i.e.*, wire fraud, in violation of 18 U.S.C. § 1343.

The Flow of Funds

34. Subsequent analysis indicates that a portion of the Defendant Property in ACCOUNT-1 can be traced to the transfers from Victim-1’s Coinbase account.

35. The one (1) transfer from Victim-1's account at Coinbase.com is reflected in Figure 1 below, with final validation times shown in UTC¹²:

Date: 03-13-2024 01:48 PM
Amount BTC: 1.33272285
Sent to wallet address: 1KmgC5oPi652sgHz5MByq9AulpnKwtPj9D (Wallet ending in 9j9D)
Transaction Hash: 48388dd0482ae39ef56d8cd39374f7aa1a33fc347ce4ddbc66564379a6a628ea

Figure 1

36. After receiving 1.33272285 BTC in Victim-1's funds on March 13, 2024 (see Figure 1), the controller of **wallet address ending in 9j9D** remitted approximately 1.2401626 BTC of the funds to **wallet address ending in HKb1S**.

37. A listing of these transactions can be found in Figure 2 below, with times shown in UTC:

Date: 03-13-2024 1:48 PM
Amount BTC: 1.2401626
Sent to wallet address: 1FUWzwzKq7G7Q2FTNvxNQYmJFxAmcHKb1S (Wallet ending in HKb1S)
Transaction Hash: c903bb557e868f2a484e7a49b3ce40978ab7eb9ea326ce165f98ade70e01c3bb

Figure 2

The Flow of Funds to ACCOUNT-1:

38. After receiving approximately 1.33272285 BTC traceable to Victim-1's funds, the controller of wallet address ending in **9j9D** remitted the funds to an intermediary wallet before ultimately transferring to the Account 1 **wallet address HKb1S**. I later contacted Binance for information relating to the transfer of Victim-1's funds into **wallet address HKb1S** and obtained account records from Binance indicating this transaction corresponds to ACCOUNT-1, as described more fully in paragraph 39 below. Intermediary wallets are typically

¹² UTC is Universal Time Coordinated, also known as Coordinated Universal Time. This is also known as Greenwich Mean Time.

private wallets or non-exchange wallets that obfuscate transactions on the Blockchain.

Intermediary wallets support the movement of illicitly obtained funds as they help to conceal and disguise the source of the BTC by layering and severing straight line coordinates of transaction activity on the Blockchain to cash out exchangers.

39. A listing of the transactions to the intermediary wallets involving Victim-1's funds can be found in Figure 3 below, with times shown in UTC:

Date: 03-13-2024 01:48 PM
Amount BTC: 1.33272285 BTC
Sent to wallet address: 1KmgC5oPi652sgHz5MByq9Au1pnKwtPj9D (Wallet ending in 9j9D)
Transaction Hash: 48388dd0482ae39ef56d8cd39374f7aa1a33fc347ce4ddbc66564379a6a628ea
Date: 03-13-2024 01:48 PM
Amount BTC: 1.2401626 BTC
Sent to wallet address: 1FUWzwzKq7G7Q2FTNvxNQYmJFxAmcHKb1S (Wallet ending in HKb1S)
Transaction Hash: c903bb557e868f2a484e7a49b3ce40978ab7eb9ea326ce165f98ade70e01c3bb

Figure 3

40. A visual depiction containing the transfers identified in Figures 1 through 3 above, are reflected in Attachment A.

41. After reviewing Attachment A and other facts of this investigation, I was able to identify that after an intermediary transfer 1.2401626 BTC traceable to Victim-1's funds were ultimately transferred to **wallet address ending in HKb1S** (referenced in paragraphs 35 and 37). I contacted Binance for information relating to these transactions of Victim-1's funds into **wallet address ending in HKb1S** and obtained account records for one Biance account. The Binance records reflect that the transfers of Victim-1's funds into **wallet address ending in HKb1S** (referenced in Figures 1 through 3, Attachment A, and paragraphs 38 and 39) is attributable to Binance account user ID number XXXXX3280, also known as the ACCOUNT-1, is held in the name of AVWEROSUO OMOKRI. The records include the email address

johnrichie513@gmail.com and Nigeria passport bearing the name of AVWEROSUO OMOKRI. ACCOUNT-1 was opened on or about May 6, 2021. In April, 2024, ACCOUNT-1 held approximately 13.99253462 BTC.

Money Laundering

42. The scam detailed in this affidavit is consistent with a criminal organization employing an emerging fraud trend involving promises of high returns in cryptocurrency investments, coined as “Pig Butchering.” This type of scheme often begins with scammers sending a victim a message, initiating contact through various social media platforms like LinkedIn, Match.com, and Facebook. The scammers then quickly establish a personal relationship with the victim or conveys a sense of expertise in investing, using emotionally manipulative tactics similar to those used in online romance scams.

43. The scammers will use elaborate storylines to convince the victim into believing they are in a relationship and or claiming to be an expert in investing. Once the victim reaches a certain point of trust, they are brought into a cryptocurrency investment scheme and are provided with fabricated information to bolster the scheme’s legitimacy. The fabricated information includes, but is not limited to:

- a. A fake investment platform via a website or mobile application that displays fictitious investment options. In reality, the website or application has limited functionality and does not allow the user any access to a cryptocurrency wallet.
- b. Fabricated investment gains that are displayed on the investment platform website or mobile application. In actuality, the investment platform does not exist.

- c. A demand to pay the fake investment platform “taxes” or “fees” on the value of the account before they can withdraw funds (and, even if they pay these “taxes” or “fees”, the victims will be unable to withdraw the funds).

44. The scam culminates once the victim assets are stolen by the scammers. In this instance, Victim-1 was contacted by online personas who claimed to have investment experience and knowledge of lucrative cryptocurrency trading opportunities. Based on my knowledge and experience conducting cryptocurrency fraud investigations, I know that criminal organizations often operate in multiple tiers of responsibility. Most often, the individual that communicates directly with the victim is on a lower tier of responsibility in the criminal organization, whereas individuals receiving funds at the end of the scheme are those who profit the most and are typically higher in the criminal organization’s hierarchy.

45. Based on my knowledge and experience, and conversations with other investigators familiar with these types of cyber fraud schemes, the online personas that contacted Victim-1 are not likely the individual they portrayed themselves to be, but rather a persona that can and often is played by more than one person.

46. After the scammers obtain control over a victim’s funds, they often engage in money laundering for the purpose of attempting to conceal the origin of the fraud proceeds. Specifically, the scammers obfuscate linear lines of blockchain transactions, separate victim proceeds, and co-mingle victim proceeds with other funds of unknown origin, including other victim funds.

47. The organization controlling the movement of fraud proceeds also utilize private wallet addresses for the movement of cryptocurrency, which is also indicative of money laundering tactics that are used to conceal and disguise the source of originating victim funds.

Private wallets are non-custodial wallets, meaning the owner, as opposed to an exchange, application, or provider, controls the private keys and therefore all associated funding. Private, non-custodial wallets can be held in numerous forms such as, wallet applications on computers and cell phones, cold storage devices not connected to the internet, and paper wallets.

48. Additionally, the organization controlling the movement of fraud proceeds will transfer funds among wallets in transactions (or “hops”) that lack ostensible business purpose, often with several hops occurring in rapid succession, which further establishes probable cause to believe that the transfers were coordinated and intended to obscure the control, ownership, source, and purpose of the funds involved in said transfers.

49. A review of the transactions involving Victim-1’s funds demonstrates that the organization controlling the wallets displayed tactics typically used in money laundering operation as described above. For example, Victim-1’s funds were transferred to a private intermediary wallet for no ostensible business purpose and co-mingled with funds from unknown sources. Victim-1’s funds were also moved at a rapid pace (within less than ten minutes) from the intermediary wallet to ACCOUNT-1.

50. Additionally, a review of Binance account records shows that ACCOUNT-1 had approximately 4 approved phones with distinct device names that do not match the name or identification documentation of the account holder of ACCOUNT-1. These are devices that have accessed the account. The use of multiple devices, not associated with the name of the account holder, to access an account is indicative of money laundering, as criminal organizations will often have one member of the group set up an account utilizing their identification documentation for KYC to obtain access to the platform account. Once the access is obtained,

the account will be shared amongst several different devices, by different group members who have different roles in the organization, much like the use of money mules.

51. A review of the deposit history of ACCOUNT-1 shows further activity indicative of money laundering. For example, the account received tokens from cryptocurrency addresses associated with fraud reports found in law enforcement databases. A search of Internet Crime Complaint Referral Form through the Internet Crime Complaint Center yields at least two fraud reports associated with the intermediary wallets through which Victim-1's funds were transferred, and an additional four complaints involving "TOM SHELDON HALEY" and the "Trade Propel" website that Victim-1 was instructed to utilize. In addition, Coinbase provided records that show additional victims have sent funds to the same intermediary wallet to which Victim-1 was directed to send her funds.

52. I have identified additional potential fraud victims who believed they invested in Trade Propel at the direction of "TOM SHELDON HALEY". Between February 2024 and March 2024, Victim-2 sent BTC then valued at approximately \$29,000 and Victim-3 sent BTC then valued at approximately \$35,000 to the same intermediary wallet (ending in 9j9D) as Victim-1. Victim-4 was also instructed by "TOM SHELDON HALEY" to invest in Trade Propel, and although funds ended up in ACCOUNT-1, a different intermediary wallet address was used. Refer to Figure 4 which illustrates the flow of funds for Victim-4's funds to ACCOUNT-1.

Date: 02-10-2024 08:18 AM
Amount BTC: .52914208
Sent to wallet address: bc1qvtw8t0arapy0tyz85jh5pse00rzspst5l8l2y (Wallet ending in l8l2y)
Transaction Hash: 6dd966d09082eb0b5cd570a8bcfa7fc57220b0ea64c080f6e7fb68af1691d5a8
Date: 02-10-2024 10:56 AM
Amount BTC: .52861163
Sent to wallet address: bc1qfw425e7apapmnzndlckdkvsrqs3rxmtwsv7s (Wallet ending in wsv7s)
Transaction Hash: bd474ce1ac92cdfd3a40aa3f4d375f155fa20224de5b6f7ed0d87eace0f54b65
Amount BTC: .00048581
Sent to wallet address: bc1qx79cmymctfwfyf6whmvl5sz0l9cr0xm370ruwvk (Wallet ending in ruwvk)
Transaction Hash: bd474ce1ac92cdfd3a40aa3f4d375f155fa20224de5b6f7ed0d87eace0f54b65
Date: 02-11-2024 08:20 AM
Amount BTC: .72415050
Sent to wallet address: 1FUWzwzKq7G7Q2FTNvxNQYmJFxAmcHKb1S (Wallet ending in HKb1S)
Transaction Hash: 96b939748dad29620c7fe0741e23441857833c38d035cdd880417984a394b42e
Amount BTC: .09331072
Sent to wallet address: bc1qfw425e7apapmnzndlckdkvsrqs3rxmtwsv7s (Wallet ending in wsv7s)
Transaction Hash: 96b939748dad29620c7fe0741e23441857833c38d035cdd880417984a394b42e

Figure 4


53. Between February 11, 2024 and May 9, 2024, ACCOUNT-1 received multiple deposits totaling approximately 12,3116 BTC, including 1.33272285 BTC traceable to proceeds from the fraud perpetrated against Victim-1.

CONCLUSION

54. Based on my knowledge, training, and experience, and the foregoing information set forth in this affidavit, I believe there is probable cause that the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) because it represents proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud) and is property involved in violations of 18 U.S.C. § 1956 (Money Laundering), or property traceable to such property.

Pursuant to 28 U.S.C. § 1746, I declare under penalties of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 16th day of February, 2025.

Respectfully submitted,



Special Agent Katrina P. Caulfield
United States Secret Service

ATTACHMENT A

